WHAT IS CLAIMED IS:

1. A method for delegation of security procedures to a second domain comprising:

generating a first key for a mobile node;

storing the first key at the mobile node and at a home domain of the mobile node;

moving the mobile node to the second domain;

sending a request from the second domain to the home domain to authenticate the mobile node;

generating a second key at the home domain using the first key and a random number and sending the random number and the second key to the second domain;

sending the random number to the mobile node by the second domain;

generating the second key by the mobile node using the random number and the first key; and

using the second key for at least one authentication procedure between the mobile node and the second domain.

2. The method of claim 1, wherein the second domain is a visited domain.

3. The method according to claim 1, wherein the authentication procedure is a key derivation procedure.

4. The method according to claim 3, wherein the key derivation procedure comprises generating at least one session key using the second key.

5. The method according to claim 1, wherein the authentication procedures comprise authentication of the mobile node by the second domain.

6. The method according to claim 1, wherein the authentication procedures comprise authentication of the second domain by the mobile node.

7. The method according to claim 1, wherein the authentication procedures comprise control by the second domain of key distribution between the mobile node and entities in the second domain.

8. The method according to claim 1, wherein the authentication procedures comprise ciphering and integrity protection of messages between the mobile node and an entity in the second domain.

9. The method according to claim 1, wherein the authentication procedures comprise distribution of dynamic keys between the mobile node and entities in the second domain based on a local security association.

10. The method according to claim 1, further comprising generating the second key at the home domain using the first key and the random number as inputs to an algorithm.

11. The method according to claim 1, further comprising sending the random number and the second key to the second domain across a secure channel.

12. The method according to claim 1, wherein the home domain comprises an Authentication Authorization and Accounting (AAA) server.

13. The method according to claim 1, wherein the second domain includes an Authentication Authorization and Accounting (AAA) server.

14. The method according to claim 13, further comprising communicating with the mobile node by the AAA server through an AAA client.

15. The method according to claim 14, wherein the AAA client comprises one of an attendant located in a router, a Registration Agent, and a server located in the second domain.

16. The method according to claim 14, further comprising sending the random number and the second key to one of the AAA server and the AAA client.

17. The method according to claim 1, wherein the second key is a temporary shared key (TSK).

18. The method according to claim 1, further comprising:

generating a second random number at the home domain;

generating a third key at the home domain using the first key and the second random number, and sending the second random number and the third key to the second domain; and

sending the second random number to the mobile node by the second domain.

19. The method according to claim 18, wherein the generating the third key is based on home domain policies.

20. The method according to claim 18, further comprising updating the second key with the third key in the mobile node.

21. The method according to claim 18, further comprising:

generating a network authentication request by the mobile node and sending the network authentication request to the second domain;

generating a first authentication response by the second domain using the third key and the network authentication request and sending the network authentication response to the mobile node;

generating the third key by the mobile node using the first key and the second random number;

generating a second authentication response by the mobile node using the third key and the network authentication request;

comparing the second domain generated first authentication response with the mobile node generated second authentication response, authenticating the second domain by the mobile node if the second authentication response and the first authentication response compare, and indicating to the second domain that the second key has been updated with the third key if the first authentication response and second authentication response compare; and

using the third key by the second domain for the authentication procedures between the mobile node and the second domain.

22. The method according to claim 21, further comprising sending a report to the second domain that the second key has been updated.

23. The method according to claim 18, wherein the third key is a temporary shared key (TSK).

24. The method according to claim 20, further comprising:

generating a third random number by the second domain and sending the third random number to the mobile node;

generating second authentication data by the mobile node using the third random number and the third key and sending the second authentication data to the second domain; and

using the second authentication data by the second domain to verify that the mobile node has updated the second key with the third key.

25. The method according to claim 24, further comprising sending a report to the home domain that the second key has been replaced with the third key.

26. The method according to claim 1, further comprising:

using the second key to generate first authentication data by the mobile node;

generating a host challenge to authenticate the home domain and sending the first authentication data, the host challenge, and a mobile node identity from the mobile node to the second domain;

sending the first authentication data, the host challenge and the mobile node identity from the second domain to the home domain;

generating second authentication data, using the host challenge and the first key, at the home domain;

sending the second authentication data from the home domain to the second domain, the second domain forwarding the second authentication data to the mobile node; and

using the second authentication data to verify the home domain by the mobile node.

27. A method for delegation of security procedures to a second domain comprising:

sharing a first key with a mobile node and at least one server in the home domain of the mobile node;

moving the mobile node into the second domain;

requesting authentication of the mobile node by the home domain;

generating a second key using the first key in the home domain;

sending the second key to the second domain; and

using the second key for at least one authentication procedure between the mobile node and the second domain.

28. The method according to claim 27, wherein the second domain is a visited domain.

29. A system for delegation of security procedures to a visited domain comprising:

a home domain, the home domain containing at least one server;

a mobile device, the mobile device sharing a first key with one at least one server in the home domain; and

a second domain, the second domain containing at least one second server, a security association existing between the one at least one server in the home domain and one at least one second server in the second domain,

wherein when the mobile device roams into the second domain, the second domain requests authentication of the mobile device by the home

domain, the one at least one server generating a second key using the first key and sending the second key to the second domain, the second key being used for at least one authentication procedure between the mobile device and the second domain.

30. The system according to claim 29, wherein the one at least one server comprises an Authentication Authorization and Accounting (AAA) server.

31. The system according to claim 29, wherein the one at least one second server comprises an Authentication Authorization and Accounting (AAA) server.

32. The system according to claim 29, wherein the mobile device comprises a mobile phone.

33. The system according to claim 29, wherein the second key is a temporary shared key (TSK).

34. The system according to claim 29, wherein the key derivation procedures comprise generating at least one session key using the second key.

35. The system according to claim 29, wherein the authentication procedures comprise authentication of the mobile device by the second domain.

36. The system according to claim 29, wherein the authentication procedures comprise authentication of the second domain by the mobile device.

37. The system according to claim 29, wherein the authentication procedures comprise control by the second domain of key distribution between the mobile device and entities in the second domain.

38. The system according to claim 29, wherein the authentication procedures comprise ciphering and integrity protection of messages between the mobile device and an entity in the second domain.

39. The system according to claim 29, wherein the authentication procedures comprise distribution of dynamic keys between the mobile device and entities in the second domain based on a local security association.

40. A method for delegation of security procedures to a second domain comprising:

moving a mobile device to the second domain, the mobile node having a home domain;

sending a second key from the home domain to the second domain for authentication of the mobile device, the second key being based on a first key shared between the home domain and the mobile device; and

authenticating the mobile device by the second domain using the second key,

wherein the second key is used for at least one of authentication procedures and key derivation procedures between the mobile device and the second domain.

41. The method according to claim 40, further comprising moving a mobile node comprising a mobile phone to the second domain.

42. The method according to claim 40, further comprising generating a session key at the second domain using the second key.

43. The method according to claim 40, further comprising:

sending a third key from the home domain to the second domain, the third key being based on the first key;

authenticating the second domain by the mobile device using the third key; and

updating the second key with the third key at the mobile device,

wherein the third key is used for the authentication procedures and the key derivation procedures between the mobile device and the second domain.

44. The method according to claim 40, wherein the second domain is a visited domain.